Notice of Allowability	Application No.	Applicant(s)	
	10/082,758	LAM ET AL.	
	Examiner	Art Unit	
	John M. Winter	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *The paper filed on December 21, 2006*.

2. ☒ The allowed claim(s) is/are *30-32,34 and 35*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

An Examiner's Amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this Examiner's amendment was given in a telephone interview with Robert Lord on March 19, 2007.

The claims are amended as follows:

Claim 30,

A method for retrieving a key value secured in a key management system comprising: receiving a request for the key value secured in the key management system; retrieving a serialized file from a key management system storage; de-serializing the serialized file producing a de-serialized file; decoding an encoded key list in the de-serialized file to produce a decoded key list; searching for a key corresponding to the key value in the decoded key list; inputting a key encryption key into the key management system; hashing the key encryption key to produce a key encryption key hash, wherein the key encryption key hash is equal to a hashed key encryption key in the de-serialized file; comparing the key encryption key hash to the hashed key encryption key in the de-serialized file to grant access to the key management system; decrypting a secret token in the de-serialized file using the key encryption key to produce at least one tuple after access to the key management system is granted; storing the at least one tuple in a data structure within the key management system; and retrieving a tuple corresponding to the key value from the at least one tuple, using the key corresponding to the key value.

Claim 34,

An apparatus for retrieving a key value secured in a key management system comprising: means for receiving a request for the key value secured in the key management system; means for retrieving a serialized file from a key management system storage; means for de-serializing the serialized file producing a de-serialized file;means for decoding an encoded key list in the de-serialized file to produce a decoded key list; means for searching for a key corresponding to the key value in the decoded key list; means for inputting a key encryption key into the key management system; means for hashing the key encryption key to produce a key encryption key hash, wherein the key encryption key hash is equal to a hashed key encryption key in the de-serialized file; means for comparing the key encryption key hash to the hashed key encryption key in the de-serialized file to grant access to the key management system; means for decrypting a secret token in the de-serialized file using the key encryption key to produce at least one tuple after access to the key management system is granted; means for storing the at least one tuple in a data structure within the key management system; and means for retrieving a tuple corresponding to the key value from the at least one tuple, using the key corresponding to the key value.

Allowable Subject Matter

Claims 30-32, and 34-35 are allowed over the prior art record.

The following is an examiner's statement of reasons for allowance:

The closest prior art of record Stein (US Patent 6,370,250) teaches a transaction network that simplifies transactions. Akiyama (EP 1 041 767 A2) teaches a system for authenticating data send to a certified system. PGP Freeware Users Guide version 7.0 teaches a system public key encryption.

What they fail to teach or suggest:

As per claims 30 and 34,
none of the art of record, taken individually or combination disclose at least the steps/components of :
decoding an encoded key list in the de-serialized file to produce a decoded key list; searching for a key corresponding to the key value in the decoded key list; inputting a key encryption key into the key management system; hashing the key encryption key to produce a key encryption key hash, wherein the key encryption key hash is equal to a hashed key encryption key in the de-serialized file; comparing the key encryption key hash to the hashed key encryption key in the de-serialized file to grant access to the key management system; decrypting a secret token in the de-serialized file using the key encryption key to produce at least one tuple after access to the key management system is granted; storing the at least one tuple in a data structure within the key management system; and retrieving a tuple corresponding to the key value from the at least one tuple, using the key corresponding to the key value ..

Even if the features missing from the above cited prior art were found in a reasonable number of references a person of ordinary skill in the art at the time of the invention would not have been motivated to combine these reference because the claimed feature of " decrypting a secret token in the de-serialized file using the key encryption key to produce at least one tuple after access to the key management system is granted;" is not a feature normally associated with key management systems and therefore would have to be disclosed by art unrelated to product distribution systems.

Claim 31 is dependant upon claim 30 and is therefore allowable for at least the same reasons.

As per claims 32 and 35,
none of the art of record, taken individually or combination disclose at least the steps/components of :
hashing the existing key encryption key producing a hashed key encryption key, wherein the hashed key encryption key is equal to a key encryption key hash in the de-serialized

file, comparing the hashed key encryption key to the key encryption key hash in the de-serialized file to grant access to a key management system; decrypting a secret token using the existing key encryption key to produce a tuple after access to the key management system is granted; encrypting the tuple using the new key encryption key producing a new secret token; hashing the new key encryption key producing a new hashed key encryption key; and serializing the new hashed key encryption key and the new secret token to produce a new serialized file.

Even if the features missing from the above cited prior art were found in a reasonable number of references a person of ordinary skill in the art at the time of the invention would not have been motivated to combine these reference because the claimed feature of "decrypting a secret token using the existing key encryption key to produce a tuple after access to the key management system is granted; encrypting the tuple using the new key encryption key producing a new secret token;" is not a feature normally associated with key management systems and therefore would have to be disclosed by art unrelated to product distribution systems.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M. Winter whose telephone number is (571) 272-6713. The examiner can normally be reached on M-F 8:30-6, 1st Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on (571) 272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

John Winter
Patent Examiner -- 3621

KAMBIZ ABDI
PRIMARY EXAMINER